Enterprise Risk Management Benchmarking Study

Evolving to an active, integrated and agile approach amidst change and disruption.
The current business landscape is pushing the limits of enterprise risk management (ERM). Companies are rightly questioning the strength of their ERM programs in the face of rapid change, competitive disruption, an unrelenting news-cycle, and a global crisis in trust. Unfortunately, this questioning may come after a major risk incident for an organization, when vulnerabilities become apparent. Despite seismic shifts in the environment and a critical need for risk agility, the evolution of ERM is slow.
This benchmarking survey illustrates current ERM practices, areas of focus, and fundamental challenges companies face in getting the attention, buy-in and support to operate and modernize their programs. Companies are still working on and struggling with the basics of ERM, which is made more challenging given a limited appetite for additional investment. Organizations may find themselves on the ‘back foot’ during a crisis in the absence of strong ERM capabilities, jeopardizing reputation, employee and customer relationships, and ultimately shareholder value.

Pragmatism rules the day, with a focus on substance (over form) and enhancing leadership and Board engagement. Most companies are working to link ERM with strategic planning and improve cross functional coordination and information flow, but this tends to be more aspirational according to our study.

What is the potential of ERM tomorrow?

Over time we’ve seen positive progress with ERM programs, shifting from a focus on process and compliance to an increasing focus on people. Although ERM executives have bigger aspirations to modernize their programs and are pushing for forward progress, budgets have generally remained static and the mood is cautious.

People at all levels of the organization drive risk through their everyday decisions and actions. As a key source of risk, people are the key to improved risk management and agility. This starts from the top, with strong leadership and board engagement, but then must permeate down beyond risk champions to first line leaders, promoting awareness, giving clarity and equipping all leaders to operate in alignment with risk expectations and appetite.

A strong culture is the thing that will move organizations from passive, point in time risk management to active, integrated and agile. This includes breaking through organizational silos, integrating critical people and processes like strategic planning, and connecting the dots across the enterprise to assemble a holistic view of risk. Data and technology will play an important role in supporting better decision-making, but won’t matter without involvement of the right people and strong information flow to ensure data is accessed and actioned.

We see the unfulfilled promise of ERM programs in an increasingly difficult and uncertain environment. ERM has the potential to contribute significant organizational value, helping organizations navigate both the opportunities and threats that risk present. In our survey, companies are making the right moves to address risk, but the question is... are they are moving fast enough?
**Benchmarking study results**

Our study showed a clear and consistent focus, across participants, on enhancing stakeholder engagement and organizational connectivity, while strengthening foundational elements of ERM programs.

The study also highlighted consistent areas of opportunity and struggle, including the use of data and technology, the application of risk appetite and tolerance and vulnerabilities related to the management of emerging risk.

| 1 | Prioritizing practical over technical |
| 2 | Connecting risk and strategy |
| 3 | Strengthening leadership and board engagement |
| 4 | Reinforcing business ownership |
| 5 | Improving cross functional risk management |
| 6 | Acknowledging data and technologies as an untapped opportunity |
| 7 | Managing with limited dedicated ERM resources |
| 8 | Struggling with application of risk appetite and tolerance |
| 9 | Acknowledging emerging risk as a vulnerability |
| 10 | Applying risk language and taxonomy |
Attention to the basics

Across benchmarked organizations, there was clear attention and desire to strengthen foundational elements of ERM, while ensuring effective use of limited resources. Although some companies in our study were actively adopting more progressive ERM practices, the majority of respondents faced constraints of investment and management appetite for change.

Companies are still working to establish and apply common risk language and taxonomies, facilitate meaningful and timely risk discussions, ensure appropriate governance structures are in place, document intelligently, and improve risk reporting. Risk registers and heat maps are commonly used to document, prioritize and report on risks. However, ERM leaders see the opportunity to reduce the administrative burden of documentation and evolve to higher-impact reporting. An annual risk assessment process is still the predominant practice, but some organizations have been able to evolve to a more continuous approach.

Getting the basics right can enable step-wise advancement of ERM programs, as illustrated by one life sciences company in the study. By establishing a global risk taxonomy, the organization improved visibility and understanding of risk through ready access to risk data at an enterprise, country, and business line level. The organization gained the ability to view risk at an aggregated and disaggregated level, aiding decision making at different levels of the enterprise.

Key Challenge: Use of Data & Technology

Although surveyed companies see great promise in better use of data and technology to support ERM, this remains an untapped opportunity for many organizations. Technology use is primarily limited to document retention and risk reporting largely through SharePoint sites. Where a GRC platform was in place, the organization realized significant benefit in holistic capture, reporting and analysis of risk data and improved visibility and decision-making. Generally, ERM leaders expressed desire to become more data driven and technology enabled but the associated costs are a barrier to adoption. While an integrated tool is on their horizon, enhanced capabilities and use of data and analytics feels like a more practical starting point.
Although many organizations have greater ERM aspirations, the following factors impact their ability to evolve: 1) Constraints of limited budgets, headcount, and appetite for change; 2) History where some programs lost credibility, being seen as bureaucratic (i.e. form over substance); and 3) The absence of a significant risk incident to draw attention to vulnerabilities.

Note that for survey participants, risk events were a key driver for re-examination of and investment in ERM programs. The programs that experienced risk events, highlighting vulnerabilities in their ERM programs, tended to have the most progressive practices, including better linkage to strategy.

Linking to Strategy
A majority of surveyed companies expressed a desire to better connect risk and strategy, often citing the 2017 COSO Guidance on Enterprise Risk Management – Integrating with Strategy and Performance. Most indicated that while their executives informally consider risk during strategic planning, ERM often didn’t have ‘a seat at the table.’ For those organizations that have integrated ERM and strategic planning, natural advancements have been made in emerging risk management and consideration of risk as not just a threat, but an opportunity.

For example, one company in our survey highlighted how considering risk as an opportunity supported the company’s strategy. The company identified a significant risk to their core servicing offering with the emergence of blockchain technology. While initially identified as a major threat, the strategic conversation evolved into recognition of a competitive opportunity. The company decided to invest in their own blockchain technology, enhancing their market position and capitalizing upon disruption in the market.

In the context of strategic planning, some respondents also described use of war gaming and similar stress testing techniques, along with advanced analytical techniques to examine risk correlations and impact on strategic priorities.

One company has been able to correlate enterprise risks to potential impacts on strategic priorities and understand risk connectivity by adopting a dynamic risk assessment approach*. This has allowed business leaders to more deeply understand top risks, the interrelationship between risks, and the impacts of risk contagion, which has improved the clarity of what they must get right and what they cannot afford to get wrong.

* A dynamic approach to risk

There are inherent limitations to a traditional risk management approach, which focuses on evaluating likelihood and impact of independent risk events. KPMG helps organizations understand risk velocity (the speed with which risk can be realized), interconnectivity, and the impact of individual risks on the broader risk network. Instead of focusing on single risk events, organizations gain a better understanding of the network of risks, and which risks have the potential to amplify risk consequences across the network (i.e. risk contagion) if not appropriately understood and addressed.

“We’re focused on if people know what their risks are and what to do about it.”
Strengthening Leadership and Board Engagement

Maintaining leadership and Board engagement is vital and continues to be a primary area of focus for surveyed companies. Half of respondents highlighted leadership engagement as an area of challenge.

ERM leaders recognize that executive leadership needs to be more than just aware of top risks, rather they need to adopt a risk mindset, model behaviors and integrate appropriate risk management (including risk taking) practices into their approach. Leaders need to “walk the talk” in order to realize the value of ERM and grow a risk-aware culture.

Respondents described a number of tactics to drive leadership engagement including concentrating effort on key leaders and influencers, evaluating the frequency and duration of risk discussions, improving reporting (e.g. dashboards and scorecards), and the formation of a dedicated risk committee.

A number of respondents described the value of a dedicated risk committee, with cross functional representation. These committees support broader risk oversight, sharing of insights, and a more integrated, enterprise view of risk. With the right composition and risk reporting methods, these committees improve leadership engagement and support execution of ERM activities within individual business units and functions.

In general, enterprise risks are being discussed by senior leaders on a quarterly cadence, with the broader support of a risk champion network. For most organizations, the Audit Committee has responsibility for risk oversight at the Board level. Board level reporting was generally semi-annual, with a focus on the top 5-10 enterprise risks inclusive of strategic risk, status reporting on priority risk response efforts, and ERM program updates for more mature programs.

Key Challenge: **Application of Risk Appetite and Tolerance**

Study participants acknowledged that while the concepts of risk appetite and tolerance are sound, they struggle with practical application. As a result, the majority of companies interviewed had not adopted these concepts. However, a few companies made progress by integrating risk appetite and tolerance into qualitative risk assessment discussions. In other words, this has enriched the dialogue on what risks are acceptable and unacceptable for decision makers. Natural linkages can be made into risk scenario and dilemmas discussions and war gaming activities.

Key Challenge: ** Emerging Risk as a Vulnerability**

While respondents acknowledged the criticality of emerging risks, especially in the current business environment, they also flagged this as a known area of vulnerability. Often these risks, like emerging technologies, new market entrants, and shifts in customer dynamics have a strong strategy component and many ERM programs are still working to get a seat at the table. Notably, ERM leaders that are connected to strategic planning expressed greater confidence in their coverage of emerging risks, realizing the benefit of these natural points of connection.

“We don’t want to be strategic or integrated, we want to be both.”
ERM leaders commonly emphasized the importance of context-rich discussions with business leaders and those involved in the day-to-day to ensure the right risks are being identified, and that those risks are being handled appropriately. However, achieving this in practice remains elusive, with continued challenges in engaging top leadership.

Leadership

Many companies equate risk culture with tone at the top because you can’t have a healthy risk culture without it. A strong risk culture starts with leaders, who are not only engaged, but actively modeling desired risk management behaviors, setting clear expectations for their teams, taking a longer-term view and showing through their actions that risk management is something all employees must embrace—not just senior leaders and risk practitioners.

Part of shifting behaviors and mindsets is ensuring that leaders are asking the right questions and encouraging active risk dialogue. For example, getting individuals across the organization to consistently consider questions like “what can go wrong?” or “how would this look in the news?” is important and healthy. Effective challenge (e.g., willingness to question, take divergent perspective) was cited as a hurdle for ERM leaders, who understand how important challenge is to strong risk management. It is all too common to hear leaders voice “That can’t happen here” or “It hasn’t happened yet, so it’s not a risk” signaling a level of complacency that needs to be discouraged and actively addressed.

80% of respondents discuss risk at least quarterly with executive leadership.
Integration

Although the ERM team plays an important role in risk culture, the heavy lifting must be done by line leaders, setting and reinforcing expectations for exhibiting a risk mindset in the day-to-day. The greatest success can be realized through cross functional partnership (e.g. leadership, ERM, HR, communications) and integrated risk management practices.

Over 50% of study participants indicated that they have been able to achieve a more holistic view of enterprise risk by improving the engagement of assurance functions [e.g. ethics and compliance, legal, quality and Environment, Health, and Safety (EHS)] in the process. This has been an effective way to involve a diversity of perspectives and achieve a more interdisciplinary approach. Programs that have taken this approach cite integration as key to their programs’ overall success and maturity.

50% felt their ERM program is integrated well with other assurance functions and the company as a whole.

Knowing and Learning

A strong risk culture requires openness and a free flow of information to foster learning and understanding. Attention should be given to sharing stories of success and lessons learned to make the impacts of risk and the connection to routine decision-making real. This is a common challenge for organizations, who: may be uncomfortable acknowledging and discussing mistakes, may struggle to make the connection between success and risk management, and/or do not have the capability or make it a priority to communicate lessons learned broadly.

The field of medicine offers good insight into how a focus on lessons learned can be operationalized to drive continuous improvement. Post-mortem reviews are conducted when negative medical outcomes occur to uncover potential root causes, while creating a climate of accountability without accusation. With the adoption of this mindset, ERM teams can play a bigger role in identifying small mistakes that have the potential to become large mistakes and taking a harder look at an organization’s culture to encourage more accountability for risk.

“If you don’t have the right governance structure then you have nothing.”
The greatest single opportunity and greatest challenge for ERM programs remains an effective risk culture, where individuals across the organization have an understanding of risk and clarity of expectations to make sound decisions and hold each other accountable in the day to day. Risk culture is about influencing behaviors and consistent execution of expectations. Risk culture is about people; it’s about addressing risk at the source every day.

It is more important than ever to get risk management right. Effective ERM will empower leaders to take the right risks, realizing significant strategic benefits (e.g. first mover advantage), support organizational agility and learning, and strengthen organizational resiliency and sustainability in a very uncertain climate.

Study results point to a spectrum of ERM practices

Common techniques

– Responsibility for monitoring risk activity and ensuring mitigation progress assigned to risk owners and coordinators.

– Aggregation of risk updates and mitigation progress are generally managed by a central ERM team/resource, who also provides constructive challenge.

– Independent evaluation of priority risk mitigation plans through the internal audit program.

– Enhancing risk reporting as a lever to improve leadership engagement.

Advancing techniques

– Leverage the financial risk management process to stress test enterprise risks.

– Maintain a central ERM function that institutes and tracks KPIs for mitigation plans.

– Partner with other assurance functions (i.e. ethics and compliance) during the risk assessment process to improve integration and gain a more holistic approach.
KPMG’s global ERM methodology and maturity framework includes leading practices and practical implementation steps. Our holistic ERM approach is designed to help organizations enhance value through an entity-wide approach to the identification, optimization, and management of the enterprise’s risk portfolio in a cost-effective manner.

We can help you to use ERM to empower strategy, performance and governance through:

– Creating a sustainable risk program, tailored to your existing culture, to proactively manage risk in a manner that protects against surprises, drives performance, and helps enable management to operate within your organization’s risk appetite.

– Identifying opportunities to improve performance, allowing you to take maximum advantage of upside opportunities by using an approach that focuses on managing risk and improving performance.

– Improving decision making and resource allocation based on the enterprise’s risk profile, risk appetite, risk connectivity, risk velocity and cost benefit tradeoffs.
Contact us

Mike Wilson  
ERM Solutions Lead  
T: 312-665-1353  
E: michaelwilson@kpmg.com

Tracey Keele  
Partner, Internal Audit & Enterprise Risk  
T: 215-990-1516  
E: tkeele@kpmg.com

David Graff  
Director, Internal Audit & Enterprise Risk  
T: 267-256-3342  
E: davidgraff@kpmg.com

Marc Silvi  
Senior Associate, GRC Technology  
T: 609-707-5888  
E: msilvi@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates and related entities.